~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JANUARY 1978

P.L. 86-36

EO 1.4.(c)

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~Classified by DIRNSA/CHCSS (NSA/CSSM 123-2)~~
~~Exempt from GDS, EO 11652, Category 2~~
~~Declassify Upon Notification by the Originator~~

~~TOP SECRET~~

CRYPTOLOG

Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

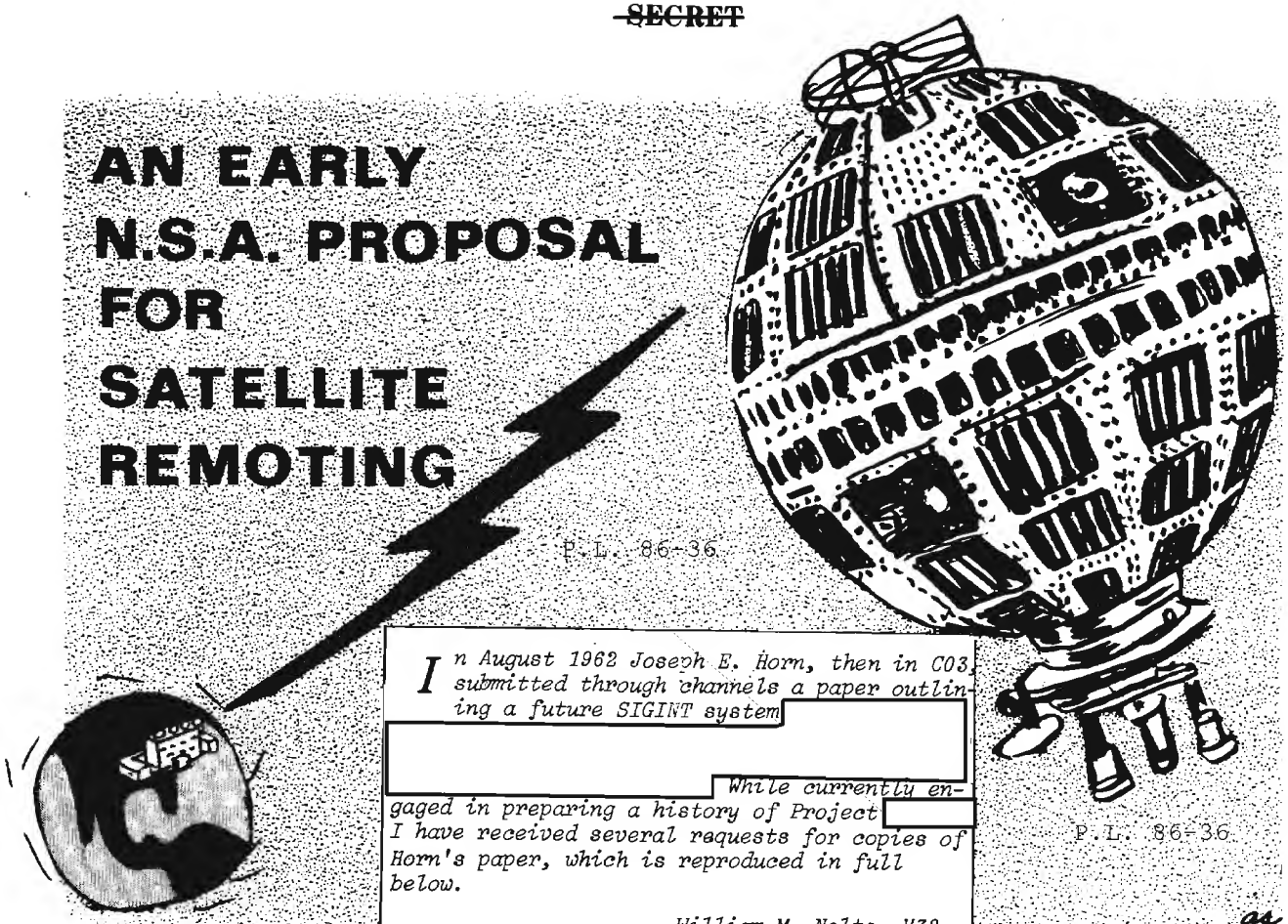
VOL. V, NO. 1 JANUARY 1978

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

~~SECRET~~

AN EARLY N.S.A. PROPOSAL FOR SATELLITE REMOTING



P.L. 86-36

In August 1962 Joseph E. Horn, then in C03, submitted through channels a paper outlining a future SIGINT system [redacted] *While currently engaged in preparing a history of Project* [redacted] *I have received several requests for copies of Horn's paper, which is reproduced in full below.*

William M. Nolte, V38

P.L. 86-36

DISPOSITION FORM

File No. C03/085/62, 19 September 1962

The attached paper is submitted, as a think piece, not a proposal. The devotion of time to considering the statements made in the inclosure was motivated by the day-to-day pressures on SIGINT activities and the feeling that NSA should have a long range plan which steps beyond the many SIGINT development plans of varying scope that are prevalent today throughout the SIGINT Community. As far as known, the idea as presented is different from any current development plans.

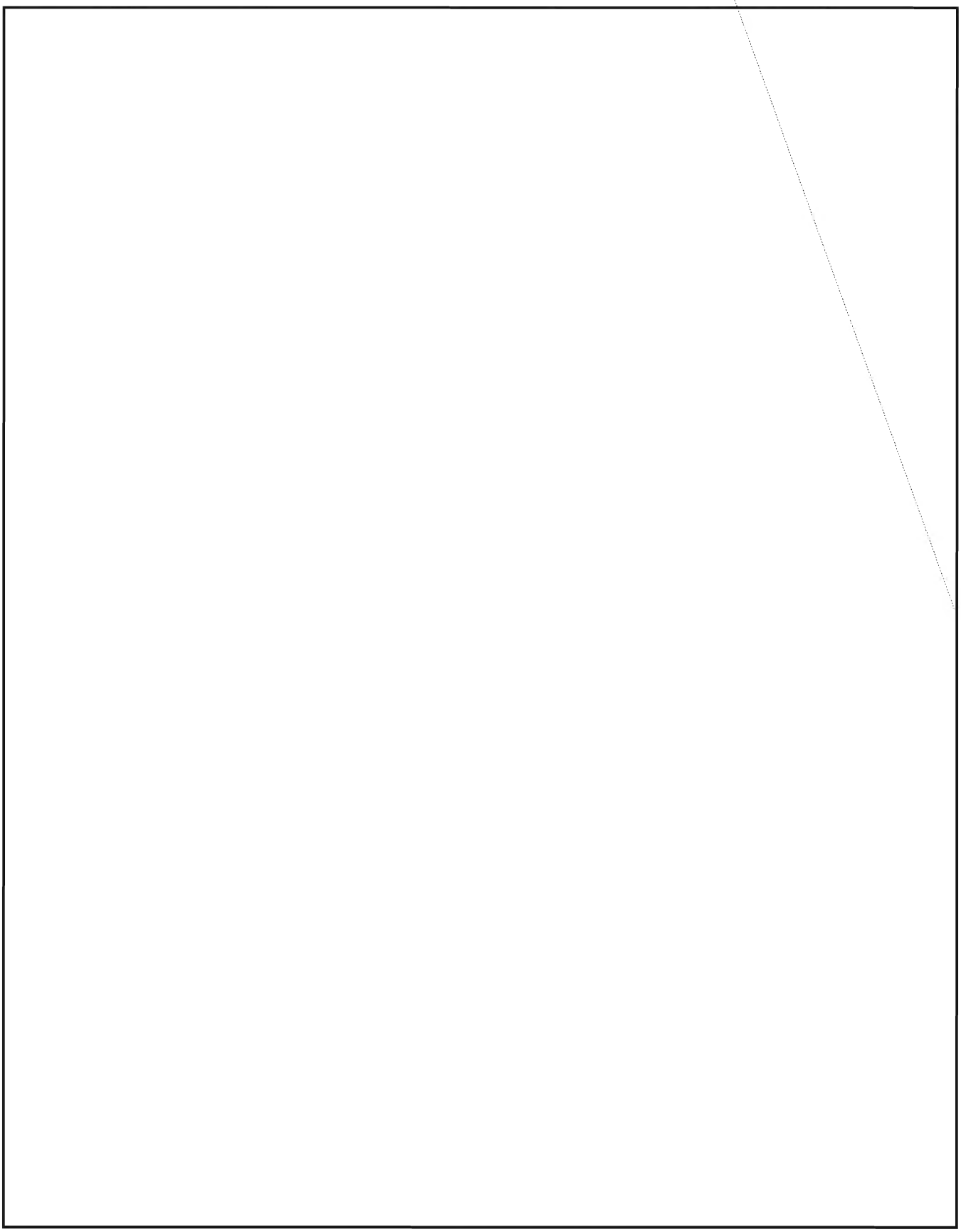
JOSEPH E. HORN
C03

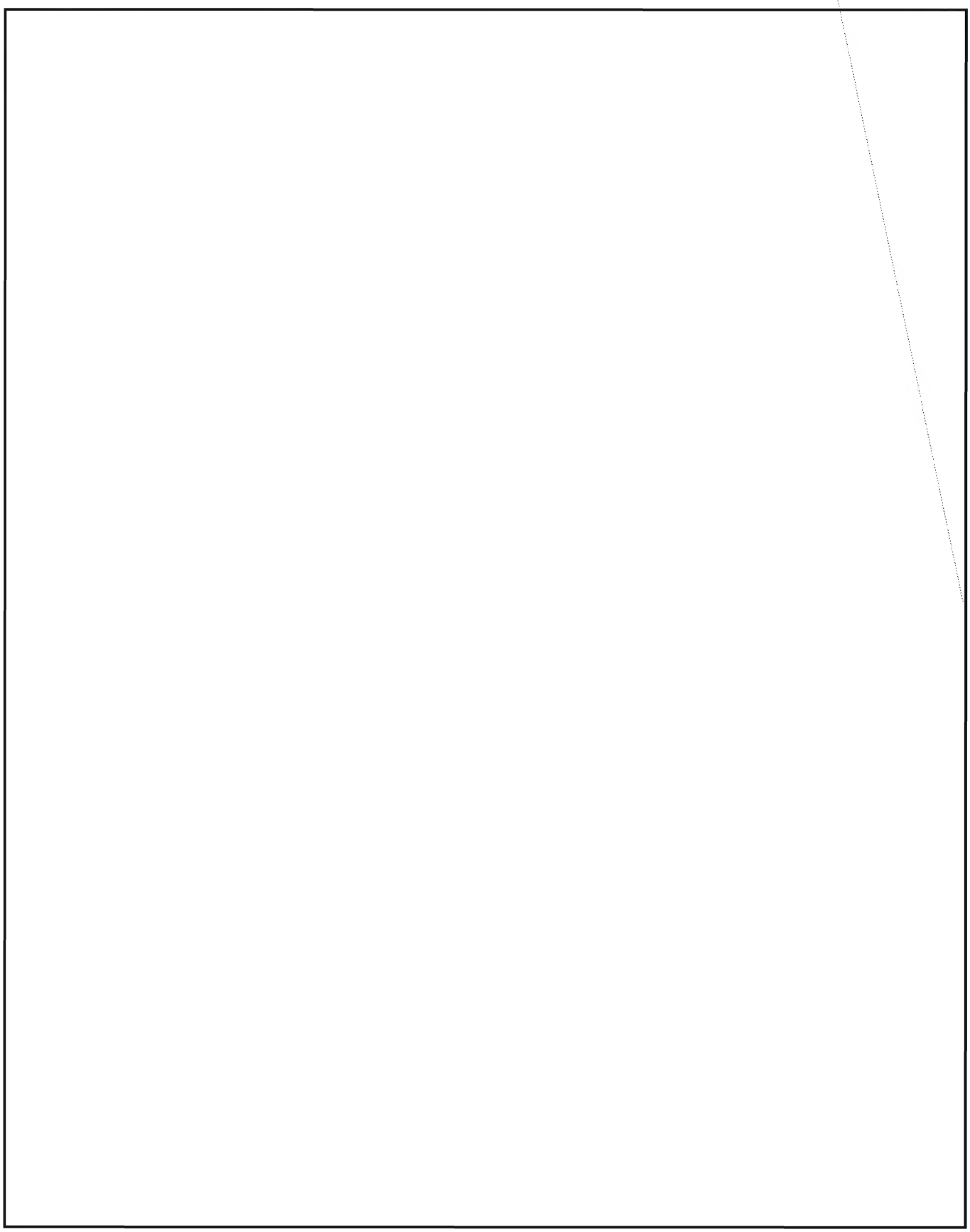
29 August 1962
JOSEPH E. HORN/Ext. 3723/C03

EO 1.4.(c)
P.L. 86-36

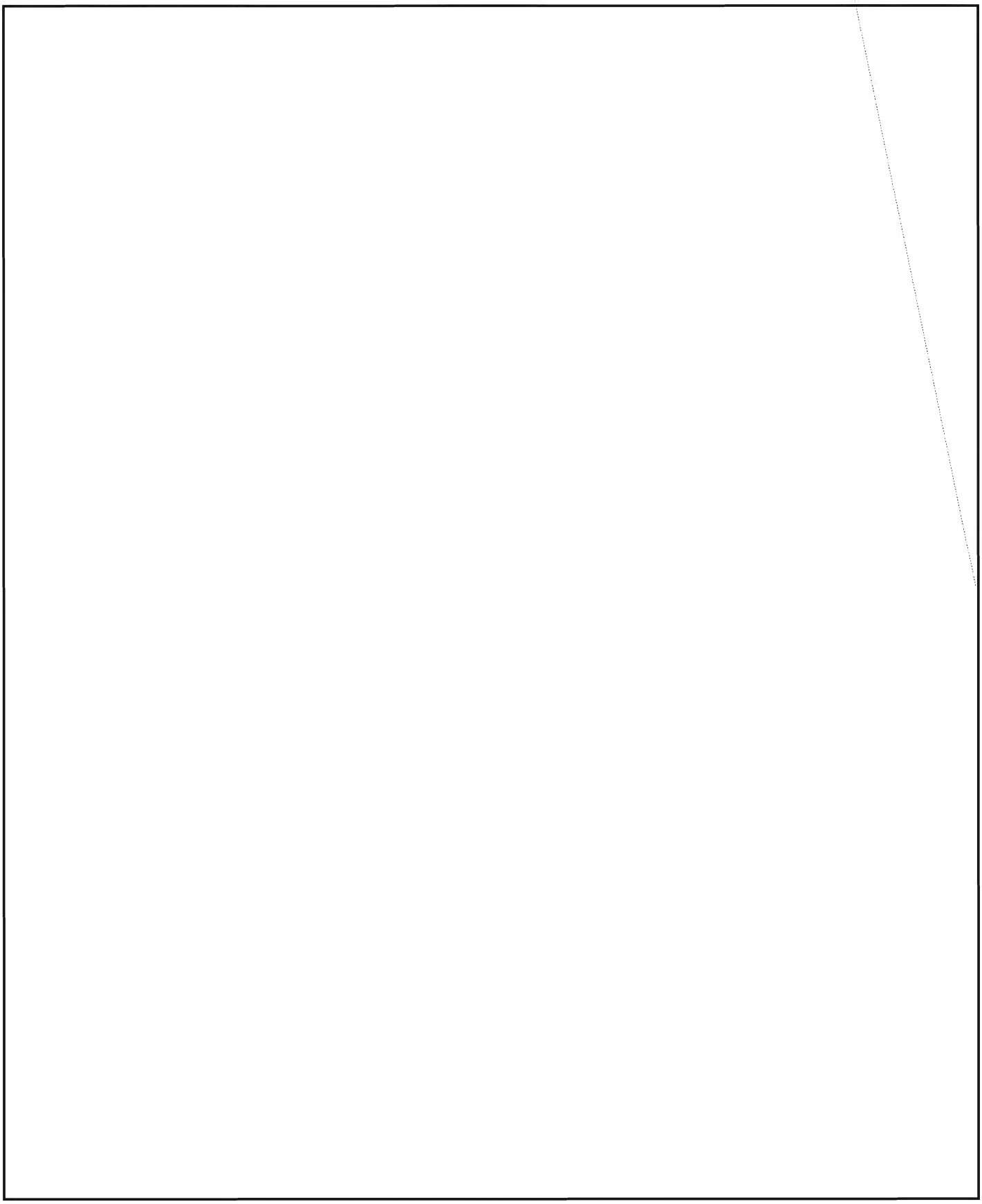
~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~





~~SECRET~~



~~SECRET~~

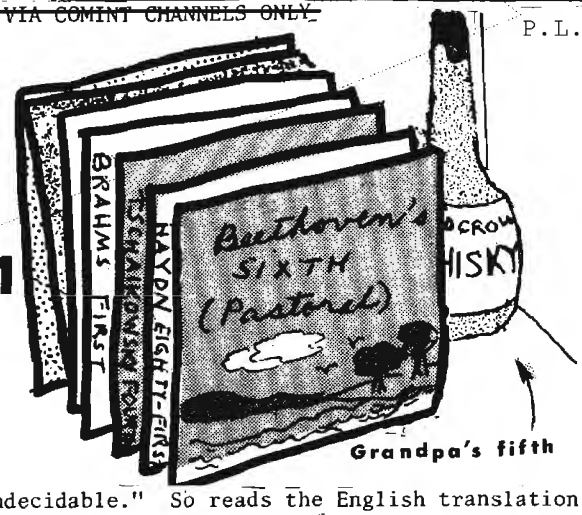
[redacted]

~~(S CCO)~~

~~CONFIDENTIAL - HANDLE VIA COMINT CHANNELS ONLY~~

COMINT, COMSEC, AND HILBERT'S TENTH

[redacted] R51



The great German mathematician David Hilbert died in 1943 after a long and highly productive career. He was well into that career in 1900 when he delivered a paper in Paris which engaged the attention and energies of mathematicians for many subsequent years. That paper[1] listed 23 problems which, in Hilbert's opinion, the mathematical community should endeavor to solve forthwith.

One by one, the 23 problems were solved, except for problem No. 10. Finally, in 1970, even that holdout gave out (or gave in). Several important blows had been delivered earlier, but the coup de grace was delivered by a 23-year-old native of Leningrad, Yu. V. Matiyasevich*.

The American mathematician Martin Davis, who had delivered, in 1953[2], one of the earlier blows, had pointed out[3] that the tenth problem was the only one of Hilbert's 23 which, in today's terminology, could be classed as a "decision" problem. Indeed the M solution[4] asserts that Hilbert's tenth problem is "algorithmically undecidable." So reads the English translation of his first Russian paper[5] on his solution. In what I assume is his own English-language paper[6], delivered at the Nice International Congress of 1970, he simply calls Hilbert's tenth problem "unsolvable." Unfortunately for those who translate from Russian to English, the English words "undecidable" and "unsolvable" are translations of the same Russian word *nereshimyj*, which is related to the Russian word *reshenie*, and that word can be rendered correctly into English, depending upon context, as "decision," "determination," "judgment," "decree," "verdict," "solution," "answer," "conclusion," etc.[7]

Of possible interest [redacted] is *not* Hilbert's tenth problem, per se, or its final alleged solution, per se. What *is*, or might be, of interest is one of the ancillary conclusions tossed off by M, first in a parenthetical note in his first paper, then in its own sentence in his 1970 paper: "For example, the set of all prime numbers coincides with the set of all positive values of some polynomial with integer coefficients!" (M's!)

*Russian spelling Ю. В. Матиясевич (pronounced "mah-tee-yah-*SEH*-vitch," with the sole stress on the fourth syllable. The name appears in the literature in the "international" transliterated form: Ju. V. Matijasevič. Henceforth I will refer to that bright kid (now an over-the-hill 30-year-older) as M.

It's been established that a polynomial in *one* variable will never generate all the prime numbers. M, however, is not talking about polynomials on one variable. His first paper gives a step-by-step *construction* of the polynomial which generates all, and nothing but, the primes (as its *positive* values). That polynomial, says M in his third paper, would have a hundred variables. By the second paper, the claim is for some 25 variables. Finally, the third paper gives the *construction* of a polynomial of 37th degree in 24 variables. That was in the first sentence of the original paper. In the addendum (added in the translation to English[8]), M is down to a polynomial of degree 21 in 21 variables. In that same paper, M goes on to say that "The number of variables may be reduced even more, but the author has been able to do this only at the expense of an essential increase in the degree of the polynomial."

[redacted]

Way back in November 1976, Whitfield Diffie and Martin E. Hellman (henceforth referred to as D-H) wrote an invited paper, "New Directions in Cryptography."[9] The ideas of these two Stanford University professors were discussed by Martin Gardner in the Mathematical Games department of the August 1977 issue of *Scientific American*. Gardner notes that the D-H thesis has been "improved" by the three M.I.T. workers Ronald Rivest, Adi Shamir, and Leonard Adleman. The nub of their improvement was the utilization of *prime numbers*. Almost simultaneously, the computer-encryption waters were further muddied by the outpourings of Gina Bari Kolata in the July 29, 1977 issue of *Science* (Vol. *197*, No. 4302), writing, in the "News and Comments" section, on "Computer Encryption and the National Security Agency Connection."

[redacted]

Annotated Bibliography

[1]D. Hilbert, *Gesammelte Abhandlungen*, Band 3, Berlin (1935). In the NSA library, the call number is: QAS, H54, 1970, V.1. See pp. 290-329 (particularly p. 310).

[2]Martin Davis, "Arithmetical Problems and Recursively Enumerable Predicates," *Journal of Symbolic Logic*, *18*, 33-41 (1953). The NSA file of this journal goes back only 20 years, but our library's [redacted] can (and already has been able to) borrow the Library of Congress copy. P.L. 86-36

[3]Martin Davis, *Computability and Unsolvability*, Wiley, New York (1958). In the NSA library, the call number is: QA 248.5, D29.

[4]Yu. V. Matiyasevich, "Diofantovost' perechislimykh mnozhestv" (The Diophantine Nature of Enumerable Sets), in *Doklady AN SSSR* (Papers of the USSR Academy of Sciences), *191*, 2, 279-282 (1970). Not in NSA Library. M's own abstract can be found in review 7A80 in *Referativnyj zhurnal: Matematika* (Abstracts Journal: Mathematics), in the R5 library -- see [redacted]

[5]Ju. V. Matijasevič, "Enumerable Sets Are Diophantine," *Soviet Math. Dokl.*, *11*, No. 2, 354-358 (1970). English version of [4]. In NSA Library, look under "Soviet Mathematics." EO 1.4.(c) P.L. 86-36

[6]Ju. V. Matijasevič, "Diophantine Representation of Recursively Enumerable Predicates," *Actes, Congrès intern. math.*, 1, 235-238, Paris (1971). NSA Library call number for the first volume of proceedings of the 1970 Nice Congress is QA1, In 8, 1970, V.1.

[7]*Russian-English Dictionary* (chief compiler A. I. Smirnitsky), Moscow (1958). There are later editions -- this is the one on my desk.

[8]Ju. V. Matiyasevich, "Diophantine Representation of the Set of Prime Numbers," *Soviet Math. Dokl.*, *12*, No. 1, 249-254 (1971). In NSA Library, look under "Soviet Mathematics."

[9]Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," *IEEE Transactions on Information Theory*, *IT-22*, 6, 644-654 (1976).

M has published frequently, almost always in Russian, since 1967. For an Englishman's reviews of the Russian originals of [4] and [8], as well as M's detailed proof of his thesis (in *Izv. AN SSSR* (News of the USSR Academy of Sciences, *35*, 3-30 (1970)), see three reviews by J. W. S. Cassels, Cambridge, England, all in our *Mathematical Reviews (MR)*, in the NSA Library: EO 1.4.(c) P.L. 86-36

MR 41, review 3390 (1971)
MR 43, review 54 (1972)
MR 43, review 1921 (1972).

M's initial paper received a favorable review by one of the Americans he cited, Martin Davis, in *MR 50*, review 6820 (1975), and M has coauthored two papers with another American he cited, Julia Robinson. The relevant reviews are: *MR 52*, review 8033 (1976) and *MR 53*, review 10566 (1977).

~~(C - CCO)~~

UNCLASSIFIED

*Addendum

The text of my original paper, as submitted to CRYPTOLOG on 28 September, ended at this point. Three weeks later, [redacted] another -- and far more competent -- R51 mathematician, brought to my attention (i.e., showed me) a 1976 P.L. 86-36

article[10] which actually contained a prime-representing polynomial. This polynomial is of degree 25 in 26 variables. The four authors assert that, "When nonnegative values are substituted for the variables, the positive values of (1) coincide exactly with the set of all prime numbers. . . [It] also takes on negative values, e.g. -76."

To assuage the reader's curiosity, I include here polynomial (1) from that paper:

$$(1)\quad (k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)\cdot(h+j)+h-z]^2-[2n+p+q+z-e]^2$$
$$-[16(k+1)^3\cdot(k+2)\cdot(n+1)^2+1-f^2]^2-[e^3\cdot(e+2)(a+1)^2+1-o^2]^2-[(a^2-1)y^2+1-x^2]^2$$
$$-[16r^2y^4(a^2-1)+1-u^2]^2-[((a+u^2(u^2-a))^2-1)\cdot(n+4dy)^2+1-(x+cu)^2]^2-[n+l+v-y]^2$$
$$-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2-[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2$$
$$-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}$$

[10]James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens, "Diophantine Representation of the Set of Prime Numbers," *The American Mathematical Monthly, 83,* 6, 449-464 (1976). (U)

Addendum$_2$

A few remarks about *the* polynomial -- call it P(a,b,...z), since it is a function of those 26 variables. Notice that P can be written in the form $(2 + k)\cdot(1 - S)$, where S is a function (of those same 26 variables) taking the very specific form of a sum of 14 perfect squares, i.e.,

$$S = \sum_{\alpha=1}^{14} T_\alpha^2,$$

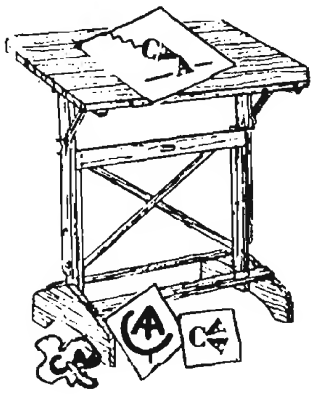
with each of the 14 T_α being a sum, difference, or product of integer variables, each occasionally raised to a low power. Since each of the T_α is an integer (whether negative or positive), its square (T_α^2) is necessarily positive (or just zero). Hence S, being the sum of squares, is either zero (if all 14 terms are themselves zero) or positive.

The product of the necessarily positive factor $(2 + k)$ by $(1 - S)$ is itself either zero, if $S = 1$, or equals $2 + k$, if $S = 0$, or is negative. Since we are to ignore all *negative* values of polynomial P, and we're quite indifferent to its zero values, we must remain indifferent to *all* values of S except $S = 0$. Variable k, being free to roam all the positive integers, starting with zero, can certainly be zero, giving the smallest prime 2 + 0 = 2, or can equal one, giving the lowest odd prime 2 + 1 = 3 and, thereafter, must be some, by no means just any, odd number (while 2 + 3 = 5, a prime, and 2 + 5 = 7, another prime, 2 + 7 = 9, which is hardly prime). *That* k, in conjunction with the other 25 variables, must somehow serve to provide a zero value to all 14 of the terms T_α, in order for P's value to be a prime. I remind at least some of my readers that an algebraic equation with integer coefficients all of whose solutions (if any) are integers is called a Diophantine equation since they afforded such entertainment to that ancient Greek mathematician Diophantus. (U)

E.S.S.

(Any more addenda? Last chance!. . All right, then, to press! -- *Ed.*)

P.L. 86-36



C.A.A. Logo Contest

The Communications Analysis Association (CAA) is looking for a logo -- a symbol or emblem which is simple yet symbolic of the goals and purposes of the Association. We've tried a few ideas of our own, but aren't particularly pleased with anything we've come up with to date.

In order to benefit from the vast amount of creative talent available throughout the Agency, we've devised a contest to find a suitable logo.

Anyone may enter. The rules are simple:

1. Art work is not important. The concept or idea is what we're seeking.

2. All entries must be submitted (one entry per page) to the contest chairman, [redacted] DS, Room 9A181, not later than 1 March 1978. Any individual may submit more than one entry.

3. Each entry must have the name, organization, and phone number of the submitter on the back.

4. Judging will be by the Executive Board of the CAA. The judges' decision is final (naturally).

5. No submissions will be returned.

The first (and only) prize will be a gift of a book of the winner's choice, and, of course, public recognition.

(U)

THE CHANGING FACE OF N.S.A.

One of our constant readers (and almost as constant contributors) is also a pack rat. He has saved, for example, all the back issues of the Agency's *Quarterly Management Review*. Recently he compared the issue for the fourth quarter of FY73 and the issue for the second quarter of FY77, and came up with some interesting figures that he wants to submit without comment. *Ed.*

How many people are there in your COSC field today, and how has that number changed over the last 4 years? The following figures were taken from two issues (4 years apart) of the *Quarterly Management Review*. Only fields with 100 or more civilians *assigned* to them are shown.

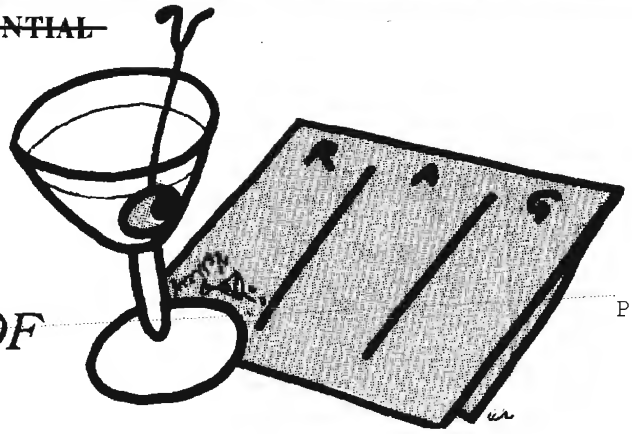
~~(C - CCO)~~

~~(S - CCO)~~

EO 1.4.(c)
P.L. 86-36

P.L. 86-36
EO 1.4.(c)

BUT WHY DO WE DO IT?



[redacted] GROF

P.L. 86-36

Every couple of months you open your copy of CRYPTOLOG and come across a piece which has as its subject matter a topic which, you proclaim to all within earshot, "everybody knows anyway." This is the January article of that species.

The purpose of this article is to point out an existing problem, briefly explore its symptoms and underlying cause, and present one means of reducing its incidence.

Picture, if you will, the following scenes:

Scene 1: George Allen and Billy Kilmer are discussing the team's faltering fortunes (or, if team loyalty will not permit it, picture Ted Marchibroda and Bert Jones). The team has just lost its eighth straight game; the QB has not completed a single pass. "But, Coach, I'm *throwing* the ball," the QB protests.

Scene 2: You enter your doctor's office for a postoperative examination; you feel just as poorly as you did before the surgery. "I've done all that I can do, Mr. Smedley; I *made* the incision," your physician says.

Scene 3: You've loaned your beautiful new 1977 Belchfire V8 to your neighbor. An hour later, you watch in horror as a tow truck returns a twisted pile of useless metal to your driveway. "It's not my fault, Harry; I *looked* both ways!"

Put you in the coach's place and you'd sack the quarterback quicker than a defensive end would. If that was your doctor, you would protest his bill, in court if need be. And, as for your neighbor, you'd probably force-feed the hood ornament to him.

But what, you ask, does all of that have to do with NSA? Those were contrived, exaggerated examples, weren't they? Yes, somewhat. But how about these:

"Don't look at me; I *sent* that tasking message."

"It's not my fault he's not here; I *called* him."

"We're covered on that; I *posted* the notice on the bulletin board myself."

"The blame lies elsewhere; I *informed* that office months ago."

"I can't help it if your in-grade is late; I *mailed* the personnel action weeks ago."

"I'm sorry the tape is blank, but I *recorded* the signal."

Do they hit a little closer to home than the first three? You bet they do! And, if anything, statements such as these are getting to be an increasingly commonplace occurrence.

The root cause of the problem is not unique to NSA, or to the federal government for that matter. It is pervasive in our society (remember the last time you spoke to the billing department at Sears?). A sociologist might point to "the attempt by an organism to adapt to an environment of increasing complexity" as the reason behind the problem. In management terms, however, the problem is due to a confusion of activities and goals.

A glance back at the scenes will highlight the problem. All the emphasized words are verbs, things that we *do*.

"I'm *throwing* the ball," "I *made* the incision," "I *looked* both ways," "I *sent* that tasking message," "I *called* him," . . .

But two self-evident statements might be made here:

Self-evident statement No. 1:

The words "doing" and "done" are *not* the same word.

Self-evident statement No. 2:

Just because someone performs an activity does *not* mean that a goal has been achieved, that the job is completed, or that that person's responsibilities have been fulfilled. The activity might have had nothing whatsoever to do with the goal. The activity may, in fact, have been *counter*productive, leaving the organization even farther from the goal than before.

What needs to be understood, then, is the difference between a *goal* and an *activity*.

A goal (or "objective," if you prefer), as generally accepted, is a state of being. It is a point or phase which is achieved or reached.

An activity, on the other hand, is something that is done in order to achieve the goal.

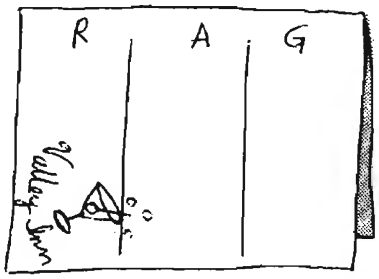
We have now come to the "so what?" point in this article. But there are actually two levels of this question -- "so what?" and SO WHAT?" -- and I'll treat them in that order.

The "so what?" is the one that you mentally utter to yourself during all meetings, briefings, tours, and conferences. While the speaker drones interminably on, listing the electronic wizardry which his organization is capable of performing or his shop's latest analytical coup, you repeat "So what?" to yourself.

At the conclusion of the gathering, and if your "so what?" has not been answered to your satisfaction, that is the time to exclaim, aloud (preferably in private conversation), "SO WHAT?"

Finally, you'll need a framework for listening to, gisting, and recalling the meeting. As with most other organizational matters, simplest is best.

The simplest model of which I am aware* is one which was developed on a cocktail napkin at the Valley Inn in Fallston, Maryland. Like another, more famous document, written on an envelope during a train ride to Gettysburg, this one retains its ability to describe many conditions while maintaining its simplicity. It is reproduced in miniature below:



R = Resources
A = Activities
G = Goals

So, during the meeting, while others are taking notes in the standard format, or merely listening, you jot down the key words in the proper cell or cells. Items such as people, equipment, time, real estate, and dollars go into the "Resources" (R) cell. Anything that will be done, such as collecting, analyzing, processing, storing, disseminating, etc., you will place in the "Activities" (A) cell. Hopefully, you will also have some "Goals" (G) to enter:

"Ten percent fewer poking errors,"

"To know the target's complete Basic Station Designator system,"

"The same hours of coverage for 22% fewer dollars,"

"A completely safe and uneventful evacuation of the crisis spot."

A simple extension of the matrix will help cover situations wherein "Time" plays a role for which you will have to account. This alteration is pictured below:

	R	A	G
P			
I			
E			

P = Planning
I = Implementation
E = Evaluation

Thus, you may:

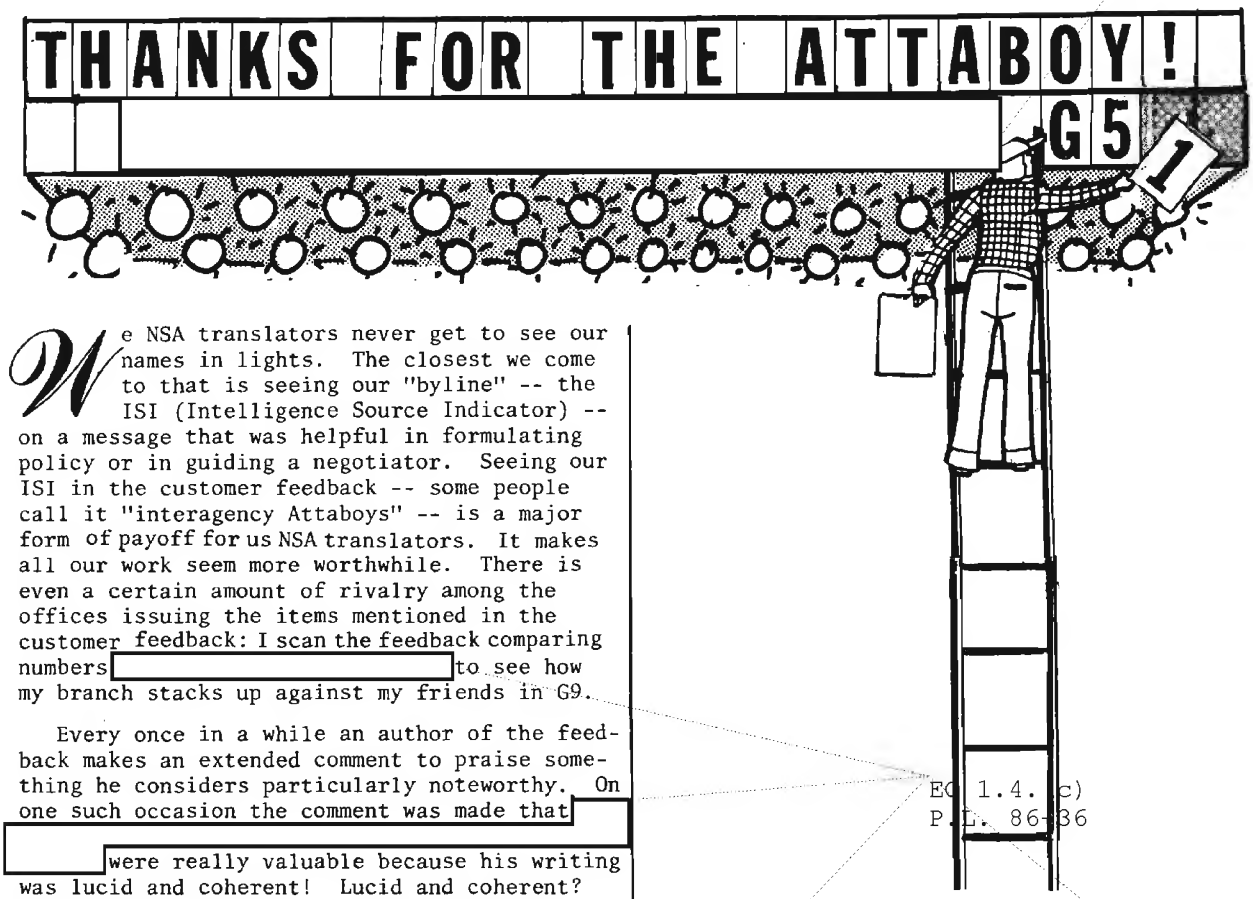
- see if the *planned* activities were actually *implemented* later on;
- determine what percentage of the *resources* were expended;
- find out if the *planned* goals, as *implemented*, were at all realistic;
- and a host of other questions (some of which may even be pertinent).

If you will enlarge the following "Program Matrix" to 8x10½" format, your division's Xerox machine will provide you enough RAGPIE matrices for a lifetime of meetings:

PROGRAM MATRIX	*Resources*	*Activities*	*Goals*
Plan			
Imple-ment			
Evalu-ate			

*J. J. Dempsey and J. A. Grant, "Viewing Program Evaluation as a Component of the Administrative Process: The RAGPIE Model," *Perspectives in Maternal and Child Health, Series B, Program Evaluation.* No. 4, September 1971.

THANKS FOR THE ATTABOY!



We NSA translators never get to see our names in lights. The closest we come to that is seeing our "byline" -- the ISI (Intelligence Source Indicator) -- on a message that was helpful in formulating policy or in guiding a negotiator. Seeing our ISI in the customer feedback -- some people call it "interagency Attaboys" -- is a major form of payoff for us NSA translators. It makes all our work seem more worthwhile. There is even a certain amount of rivalry among the offices issuing the items mentioned in the customer feedback: I scan the feedback comparing numbers to see how my branch stacks up against my friends in G9.

Every once in a while an author of the feedback makes an extended comment to praise something he considers particularly noteworthy. On one such occasion the comment was made that were really valuable because his writing was lucid and coherent! Lucid and coherent? We had always thought he was just a pain in the neck!

Then it struck me: this comment was at least as much a tribute to the skill of the translators and the checking team I ought to give a brief description of the checking process, since it represents the pinnacle of the Agency's language skill -- checkers are operationally responsible for the Agency's looking good in print.

G51 Checking Process

One very successful, efficient, and productive system for checking translations involves two stages. In the first stage, one person reads the translation aloud while a second person follows along in the original, foreign-language text. Whenever the translation differs from the meaning in the initial text, the second checker interrupts the first and gives a sight translation of that portion of the text. The two people then resolve the differences until both are satisfied. Sometimes the resolution requires considerable delving into dictionaries and glossaries and the use of a thesaurus in both languages. Occasionally it requires brainstorming with other checkers and senior translators. When a decision is finally made, the checkers may record the finding in their glossary for future reference, and resume reading the English translation.

EO 1.4. c)
P.L. 86-36

The second stage of the process is to turn the corrected translation over to a third checker who edits the English Surprisingly, this two-stage process is actually more efficient than having the three checkers work separately, and far more likely to catch errors and accurately represent the intent of the original author. The dialogue between the checkers that the process requires also satisfies the social needs of the checkers and upgrades their job satisfaction. The editing process is so important and demanding that if the Agency ever decides to solve its "language problem" by promoting operational linguists to higher grades, my vote is to promote the checkers first!

Clear to Whom?

Let's return to the business of being lucid. When an author is lucid, his meaning is completely clear. He uses grammatical constructions, figures

of speech, historical and literary allusions, etc. that he knows his reader will be familiar with. But translating a foreign text that is completely clear to the *foreign reader* does not always result in something that is completely obvious to the *English-speaking reader*. It is hard enough for the translator to make the meaning completely clear to *his* reader when a foreign word has no direct one-for-one English synonym -- if a foreign word means either "son-in-law" or "grandson," does the translator flip a coin, or put in one of those footnotes that nontranslators hate, or what? Yes, that's hard enough, but when a metaphor creates an image, the problem is sometimes compounded exponentially because the image itself is unfamiliar to Americans.

[redacted]

Challenging images like these can be exasperating, but the silver lining is that the possibility and unpredictability of their occurrence means that no computer will ever fully take over my job.

[redacted]

The absence of any one of them can leave a translator wishing that the next issue of the *NSA Newsletter* would come so that he could at least spend the government's time solving the puzzle. Since none of the three can be controlled by the translator, there is a constant threat that some change will eliminate the job of even the most skilled and dedicated professional.

EO 1.4.(c) P.L. 86-36

Perhaps that is why the "interagency Attaboys" are so welcome. Even if people in other agencies do not have a good feel for what it takes for a diplomat to be lucid and coherent, it is very reassuring to know that somebody else values our work.

~~(TSC)~~

~~CONFIDENTIAL - HANDLE VIA COMINT CHANNELS ONLY~~

Never mind what ever happened to Baby Jane, or even to the CAA!

P14 asks: What Ever Happened to COPES?

[redacted]

EO 1.4.(c)
P.L. 86-36

~~(C - CCO)~~

UNCLASSIFIED

EO 1.4.(c)
P.L. 86-36

THE MAN WHO BROKE PURPLE

REVIEWED BY **P. William Filby**

The following review appeared originally in the Baltimore Sunday Sun, October 16, 1977, under the title "Teaching Purple to Talk Saved Thousands." Its author, P. William Filby, is already known to our readers as the author of "Ultra Was Secret Weapon That Helped Defeat Nazis" (CRYPTOLOG, December 1975) and as the husband of CRYPTOLOG SRA Editor, Vera Filby.

Ed.

The Man Who Broke Purple. By Ronald Clark. 271 pages. Little, Brown. $8.95.

By virtue of recent books on cryptography, starting with "The Ultra Secret," British biographer Ronald Clark felt that the story of William Friedman, grand old man of American cryptography, should be told. It was a daunting task because the British law permitting release of certain classified information after 30 years is not matched in the United States. No doubt there were many on both sides of the Atlantic who felt that Wing Commander Winterbotham's story of the breaking of Hitler's command cipher in "The Ultra Secret" was unwise, but since the documents were 30 years old nothing could be done about the publication.

Winterbotham opened up a Pandora's box, and it was not long before we had "Bodyguard of Lies" and "A Man Called Intrepid" -- and now "The Man Who Broke Purple." The chief difficulty with all these authors is that none was actually involved in cipher work and therefore their treatment of cipher breaking is second-hand. Since those who were involved are unable (and unwilling) to assist the writers, errors were unavoidable. These books can be faulted heavily on this score, but since some of Friedman's work is public knowledge through Senate and other hearings at the time of Pearl Harbor, Ronald Clark had masses of information to use, and he make a great effort to interview those who knew Colonel Friedman. The reviewer well remembers a dinner with Mr. Clark, fresh from his triumph as the biographer of Einstein, where it was impossible to fill in any of the gaps vital to the story. But it was possible

to give some insight into Friedman as a person through a friendship which started in November 1942 and continued until his death in 1969.

Readers will be a trifle disappointed if they expect startling disclosures, but the author has done all he could to write of the man -- his many successes, his few failures, and his psychological sufferings and frequent depressions. Because of Russian pogroms, the Friedman family fled to America when William was only 3. Clark tells of his early life with its setbacks, but we find him as a young geneticist at Cornell University and later working for one Colonel Fabyan, who had a team at his Riverbank Laboratories in Illinois attempting to prove that Bacon and not Shakespeare had written the plays. All manner of tests were made on the First Folios and other Shakespearean works, but in 1957 Mr. and Mrs. Friedman exploded the whole theory in a book "The Shakespeare Ciphers Examined." Bill and Elizebeth -- she was also and still is an expert cryptographer -- made fun of all the Shakespeare cipher theories, and in fact with one system developed by a Fabyan worker Bill "proved" that he had himself written the plays.

But if Fabyan was an eccentric, he was nevertheless the cause of the two meeting and forming easily the world's finest husband and wife cryptographic team. While Friedman was with the Army, Elizebeth was with the Navy, Coast Guard and Treasury, both on similar though separate tasks and no doubt similarly successful. Certainly their later collaboration on the Shakespeare book was a brilliant achievement.

When World War II started, the Army Department quickly called upon Friedman to create a team, and through superhuman efforts the Japanese main cipher known as "Purple" was solved and in fact was being read at the time of Pearl Harbor. Purple was the name given to the diplomatic cipher system used by the Japanese Foreign Office for the most secret communications with its ambassadors abroad, and its decipherment makes exciting reading. If the reader wonders why even with Purple the Pearl Harbor defenses were unready he should study Roberta Wohlstetter's "Pearl Harbor" to realize the confusion which existed at that time. The breaking of Purple has been public property for over 30 years. With these records and with the Friedman papers in the George C. Marshall Research Foundation and invaluable help from Elizebeth Friedman, Clark tells a fine story, and even those close to William Friedman for many years will learn facts hitherto unknown to them.

Clark has given a sympathetic and penetrating study of America's outstanding cryptographer (*pace* Major Herbert Yardley and his "American Black Chamber"). Tyros will enjoy the succinct descriptions of the ciphers and their breaking since they are presented in clear, nontechnical language and no doubt were vetted by Elizebeth Friedman.

Unfortunately such men as Friedman are sworn to everlasting secrecy and their fame comes, if ever, after their death. Though he was awarded America's top civilian honors, the reasons could not be spelled out, and in fact the actual ceremonies were generally held out of the reach of the press.

Various writers have averred that the reading of Ultra and Purple and other ciphers actually won the war. There are many who will dispute this, but Clark's book will leave the reader with the certainty that even if the outcome had been the same, victory would have taken much longer to achieve without the knowledge derived from the breaking of the ciphers.

Mr. Filby is director of the Maryland Historical Society; he served in British Intelligence in World War II.

(U)

The following book review appeared originally in the Agency's COMSEC Intern Review, Vol. I, No. 1, September 1976. That publication, which is issued quarterly by the COMSEC Intern Organization, is entirely produced and managed by the interns toward whom it is oriented. In his first editorial, the founding editor, [redacted] *stated that the publication is intended as a "vehicle [of instruction] not only for the interns, but also for those in the larger COMSEC community who care about the principles, techniques, theory, and applications of COMSEC. A primary purpose of the Review, therefore, is to provide an educational tool of general COMSEC interest." For further information about the COMSEC Intern Review, call the current editor,* [redacted] *1LT USA; S02, x2445s.*

Ed.

A.C. Brown's "BODYGUARD OF LIES"

REVIEWED BY [redacted] S02

Bodyguard of Lies is called "the most important work on World War II in a quarter century" by the Army historian Charles B. MacDonald. It is a master work on strategic thinking and planning and it will surely become a recognized classic on the art of stratagem. No less than Barton Whaley, that other master of stratagem, author Anthony Cave Brown demonstrates decisively that static security measures contribute little to effective protection. Where Whaley consciously and statistically

points to this conclusion, Brown achieves more by an organized recounting of events, plans, and programs.

Besides the elaborate orchestrations of BODYGUARD and FORTITUDE, the operations and programs surrounding El Alamein are of particular interest to the COMSEC strategist and tactician. As is ever the case, the COMSEC lesson was only learned after a series of staggering military reverses, and then only after the capture of a German "wireless intelligence post." When the sources of Rommel's "brilliance" were demonstrated to be poor American and British radio security, the Allies at last reacted with swiftness and imagination. Cryptosystems were both changed and used for deception. "New disciplines were imposed for the use of radio telephones, call signs, cryptographic procedures, voice codes, wireless silences for units on the move. . . The British formed new companies to monitor the security procedures of their own troops and severe disciplinary action was taken against offenders." One of the greatest COMSEC actions against Rommel, however, was the destruction by the British of his entire experienced radio intercept organization. The new inexperienced organization was "very vulnerable to wireless deception." Not only did the British exploit this weakness by Manipulative Communications Deception (MCD), but they also reconstituted a captured German espionage net and used this fiction to pass deceptive intelligence to Rommel. All the fabrications were carefully supported by camouflage feints and leaks of material. With a fine eye for essential detail Brown relates how the "Desert Fox" was systematically turned into a dunce and carefully maneuvered into a trap.

A large portion of the book is devoted to COMSEC -- practices, systems, successes, and failures. The authoritative voice of Ultra is consistently heard throughout the work. It is the final authority on all German plans, beliefs, and intentions. This constant unfailing source of intelligence brings the weighty and cumulative conviction that this COMSEC disaster was one of the primary causes of Germany's downfall.

In sharp contrast to this strategic failure of COMSEC is the painstaking use by the British of a one-time pad to transmit the whole BODYGUARD plan, a mile long, to Moscow.

While Brown does not blanch at revealing many of the subtleties of Allied deceptive practices, he does not give cryptographic system details to any substantial degree in the methods by which cryptographic systems were broken. Some measure of this book's concern with COMSEC is indicated on page 912 in the index, where more than a full column is devoted to codes/ciphers and cryptanalysis.

One of the most fascinating chapters of the book is entitled the "Wireless Game." As D-Day approached, deceptive gambles became both more elaborate and more risky. Operators were sent into the field with ciphers "the British knew the Germans would be able to decrypt." The British would then send "normal" traffic to their operators and thereby feed the Germans deceptive information. Sometimes this program compromised numbers of agents. Brown pursues this labyrinthine aspect of stratagem. He scrutinizes its effectiveness, raises the ethical considerations, pursues the official inquiries and their muddied conclusions. The human difficulties with such operations are painfully illustrated. The decisions were made indeed, but were they as ruthless in their use of human life as some thought? He gives the benefit of doubt if such is warranted. In all he shows that men did not risk other men's lives lightly. Whether it was Churchill's decision about alerting Coventry and sacrificing ULTRA or SOE's game with Princess Khan, the ends did not easily justify the means.

In summary, *Bodyguard of Lies* is often carefully researched and entertainingly written. It is a monumental and unforgettable volume. It contains both conceptual strategic sweep and finely chosen detail. The subjects of strategy, stratagem, and COMSEC are treated in a balanced and integrated manner. It is a necessary volume for the serious COMSEC professional.

(U)

(U)

NSA-crostic No. 11

by guest NSA-crostician
David H. Williams

The quotation on the next page was taken from the published work of an NSA-er. The first letters of the WORDS spell out the author's name and the title of the work.

DEFINITIONS	*WORDS*
A. U.S. state capital (2 wds)	198 204 7 150 175 59 69
B. Testify	83 74 17 93 173 37
C. "--- Angeles"	136 91 103
D. Avid	40 99 143 26 43
E. Prepare potatoes; popular TV program	14 197 86 28
F. See Word L	147 206 195 76 129 96
G. Glowing coal	19 187 167 29 70
H. Laugh nervously	124 157 1 97 88 5
I. First pocket watch (ca. 1500) -- "Nuremberg ---"	3 52 200
J. "Point ----------"	190 152 148 172 27 105 186 214 12 130 64 94
K. Pester	145 53 71 127 48
L. Followed by Word F, Word A's state	192 166 113
M. Pertaining to a stomach ailment	24 183 107 137 179 194 131 181 110 155 32
N. Character in A. A. Milne's books (2 wds)	33 139 66 50 81 4 118 89 211 132 57 104 185 202 177 25
O. Star (prefix)	142 95 45 216 125
P. Second line of Burma-Shave jingle beginning "You know your onions..." (2 wds)	116 203 11 176 165 117 72 138 15 30 39 41 80 21
Q. Third line of jingle (4 wds)	205 98 82 141 87 67 36 60 163 169 101 215 23 85 115 9
R. Mutually existing, shared	207 128 56 108 213 13 121 210 188 174
S. Selected at random and without reason	6 170 61 114 90 31 58 22 168
T. What the Hindu holy man saw after standing on his head for 20 years ("a ------")	119 44 182 164 63 92

U. Last line of jingle (5 wds)

V. Swiss adventurer who "initiated Peter the Great into the pleasures of debauchery and became his best friend"

W. Fix

X. Miserly

Y. Set aflame

Z. Extemporaneous

Z_1. David Brinkley

8 191 73 111 178 196 20 79 55 51 34 126 38

212 140 122 134 156 16 199

189 133 42 75 47 159

171 78 209 46 151 201 62

109 162 135 160 100 68 54 35 193 144 18

102 65 77 180 153 161

208 184 120 2 10 112 158

106 146 49 149 123 154 84

1 H	2 Z	3 I		4 N	5 H	6 S	7 A	8 U	9 Q	10 Z	11 P	12 J	13 R		14 E
15 P	16 U	17 B		18 X	19 G	20 U	21 P	22 S	23 Q	24 M	25 N	26 D		27 J	28 E
29 G		30 P	31 S	32 M	33 N	34 U	35 X	36 Q		37 B	38 U	39 P	40 D		41 P
42 V		43 D	44 T	45 O	46 W	47 V	48 K	—	49 Z_1	50 N	51 U	52 I		53 K	54 X
55 U	56 R	57 N	58 S	59 A	60 Q		61 S	62 W	63 T	64 J	65 Y		66 N	67 Q	68 X
69 A	70 G	71 K	72 P	73 U		74 B	75 V		76 F	77 Y		78 W	79 U	80 P	81 N
82 Q	83 B	84 Z_1		85 Q	86 E		87 Q	88 H	89 N	90 S	91 C	92 T	93 B	94 J	
95 O	96 F		97 H	98 Q	99 D	100 X		101 Q	102 Y	103 C		104 N	105 J	106 Z_1	107 M
108 R	109 X	110 M	111 U	112 Z		113 L	114 S	115 Q	116 P		117 P	118 N	119 T	120 Z	121 R
122 U	123 Z_1		124 H	125 O		126 U	127 K	128 R	129 F	130 J	131 M	132 N		133 V	134 U
135 X	136 C	137 M	138 P	139 N		140 U	141 Q	142 O	143 D	144 X		145 K	146 Z_1		147 F
148 J	149 Z_1	150 A		151 W	152 J	153 Y		154 Z_1	155 M	156 U	157 H	158 Z		159 V	160 X
161 Y		162 X	163 Q	164 T	165 P	166 L		167 G	168 S		169 Q	170 S	171 W	172 J	173 B
174 R	175 A	176 P	177 N	178 U	179 M		180 Y	181 M		182 T	183 M		184 Z	185 N	186 J
187 G	188 R	189 V		190 J	191 U	192 L	193 X	194 M	195 F	196 U		197 E	198 A		199 U
200 I	201 W	202 N	203 P	204 A	205 Q	206 F	207 R		208 Z	209 W		210 R	211 N	212 U	213 R
214 J	215 Q	216 O													D.H.W.

(Solution next month)

[redacted] C.A.A. NEWS [redacted]

President's Letter

CAA is on the move again, energized by the deepfelt concern of its membership -- including new members, who saw in the Association the potential to meet a real need. "Professional growth" has been the objective since our by-laws were first adopted. It should be a personal objective for each of us. Under [redacted] inspired leadership this past year, the Association continued the attempt to realize that objective. Why CAA? Because, of the various groupings and mechanisms available to us, CAA is pan-discipline in its orientation. (Even collectors, who wanted a home of their own and are off to a great start with Bill Hunt and the newly formed Collection Association, continue to have a role in CAA.)

Tom has given us a vision and a challenge. As incoming President, my aim will be to further the accomplishments of this past year. Extend an invitation to your coworkers to join with us. Make a special effort to enlist professionally motivated military specialists. Attend our open Board meetings -- make your views known and lend us your support. Promote the CAA. Help us to continue our contacts with our people in field service.

An alma mater of fond memory adopted some years ago a slogan which I'd like to borrow for CAA: "Emphasis on Excellence." Let's keep that thought in front of us.

Dave Gaddy

Hurry, hurry, hurry!

(A few choice memberships still available!)

In the past few issues of CRYPTOLOG, [redacted] provided the CRYPTOLOG reader with some incisive, and often witty, perspectives into the "new" Communications Analysis Association (CAA) and the underlying philosophy that governs it.

But what exactly is the CAA? The CAA was established to promote professional growth and outstanding accomplishments in the career fields involved in communications analysis, e.g. traffic analysis (TA), special research (SR), signals collections, cryptanalysis (CA), and communications security (COMSEC). Using its interdisciplinary membership, the CAA would promote active dialogue or an exchange of ideas in an effort to stimulate the U.S. cryptologic community with new concepts in the application of communications analysis to cryptologic problems. Such an exchange of ideas is manifested in the fine lecture series sponsored by the CAA, e. g., Whitney Reed's [redacted] The CAA also sponsors technical briefings for smaller audiences and special interest groups.

Equally important to the CAA, however, is the contribution it can make to *your* professional development. The CAA is not only interested in those who have been professionalized but also those who aspire for professionalization in the career fields mentioned above. In an effort to augment existing structures within NSA, the CAA is working on an approach to "career development" for both categories of members. For the aspirant, we hope to draw on our most important asset -- our cadre of experienced, knowledgeable individuals within each discipline. We feel strongly about helping aspirants toward career professionalization. This help could be in the form of work/study groups prior to PQEs (what to look for, etc.) or more individualized tutoring, etc. For the professional, the CAA is currently thinking about and talking (with M and others) about a post-professionalization program. We envision a program that would encourage professionalized individuals to broaden themselves so that they could function more effectively within an interdisciplinary environment. Such a program could include NCS courses, university-level courses, and special training that would provide the opportunity to achieve this broad, interdisciplinary perspective.

P.L. 86-36

So, you see, the CAA is concerned about you and can provide something for you in the form of its stimulating lecture series, its special interest groups, and its real concern for your "career development program." All the CAA wants in return is to have as members concerned, dedicated individuals like yourself.

So how about it? Why not join the CAA today? Call any of the following individuals for an application form or for more information:

David Gaddy, President, 3247s

[redacted]

P.L. 86-36

[redacted]
Chairman, Membership Committee
~~(C)~~

New, new, new!

A Special Interest Group on Cryptologic History. [redacted] (4087s) is the organizer of this group, which will have had its first organizing meeting by the time you read this. If you missed that meeting, but are interested, call Bill for the latest on this new SIG.

Logo Contest

For information, see page 7.

The Editor's Page: THE JOYS AND FRUSTRATIONS OF PLURAL-DROPPING By A.J.S.

One of the easier chores of the CRYPTOLOG editor is making minor changes in the text automatically, changing, for example, "this phenomena is" to "this phenomenon is." Or changing "these antennae are" to "these antennas are."

Sometimes the original author doesn't like the change, and if, for example, he or she doesn't like my version, "these media are," we usually come to a compromise. A few months ago I automatically changed the statement "you may find these data in technical reports" to "you may find this data in technical reports." After checking the proof sheets, the author[2] told me, "I've been insisting for years that 'data' is plural, and if you print it this way, it will look as though I've finally knuckled under." So, what the heck, I changed it back to "these data," and that's how it appeared in print. (Did anyone notice, one way or the other?)

The following article, written soon after the unveiling of the mosaic NSA seal in 1968, has been awaiting the proper publication moment since then. Having recently corrected the straw that broke the editor's back, I now ordain that that moment has come.

The article contains a couple of references to since-departed Beautiful People, and at first I thought of updating the references. But then I decided that that would be a form of tampering similar to the kind that ruins old songs, as when Pearl Bailey sings, "A-washin' an' a-scrubbin' don't make me look like no movie star!" instead of "Don't make me look like no Hedy Lamarr!" Why don't we just assume that everyone knows who Hedy, and Ari, and Maria are?

Some people enjoy name-dropping, saying things like "When I was on Ari's yacht a couple of years ago, I thought Maria looked a bit peevish." Others enjoy placename-dropping. "If you think that *this* is deep snow," they say, "you should have seen the snow in Garmisch-Partenkirchen the year of the big snowslide on the Zugspitze." Still others -- it takes all kinds -- prefer plural-dropping. The plural-dropper looks up from what he is reading -- perhaps the newspaper, the *NSA Newsletter*, or an important, or at least important-looking, report -- and says, "Oh?" Having attracted the attention of those around him, he reads a phrase from the text, preferably in a colorless tone that disguises what's biting him. One of those in earshot asks, say, "What's wrong with 'This is the most important media of expression'?" The plural-dropper says simply, "Well, 'media' is plural -- 'medium' is the singular, remember?" Then he shuts up, while the others get into an emotional discussion bringing in everything from whether to say "None of them is" or "None of them are" to completely ad-hominen (fancy way of saying "Your-mother-wears-army-boots") remarks such as, "Well, maybe in your part of the country they say that, but in cultivated English we don't usually say it that way."

Well, today, I -- or, rather, a certain plural-dropper I know -- was able to read aloud one sentence from the *NSA Newsletter*, and get two with one blow. "Byzantine smalti," the sentence read, "considered the king of mosaics, is still being used to decorate modern building facades, and the NSA insignia was made with smalti in much the same way that mosaics were made when Michelangelo was painting the Sistine Chapel." "What's wrong with that?" came the nibble, "they probably don't have a cedilla to put under the 'c' in 'facades.'" "No, I was referring to 'smalti' -- pieces of glass used in making mosaics -- that's plural. 'Smalto' is the singular, remember? And, oh, by the way, 'insignia' is a plural word meaning the distinguishing signs. 'Insigne' is the singular, remember?" Then, since I have been convinced that everything happens in threes, I began to read each and every item in the *Newsletter*, looking for the third boo-boo involving singular or plural number. Twelve pages later, I found it. The item on the Fort Meade nursery said that "Parents may leave their offsprings for periods of an hour or more. Is it conceivable that someone does not know that, while "bedspring" has a plural, as in "People may leave their bedsprings to be retied," "offspring" in the sense of "progeny" is singular and collective?

Elated or not, any plural-dropper who finds three examples in a single publication is morally obligated to write an article on the problems of handling singular and plural nouns in English. Even if, ignoring the current NSA trend of using a cute title to signify a discussion of a complex and potentially dull topic, he decides not to call it "Are It Singular or Are It Plural?", he still has to mention a couple of linguistic facts of life.

[1] Well, maybe a wee bit more than a page!

[2] I have deliberately used the words "the author" instead of the appropriate "he" or she," in order to protect the author's identity. Norma would kill me otherwise.

One such fact is that there's no logical reason why English, or any other language, or any old speaker, for that matter, thinks of something as being singular or collective, rather than plural. In English we say, "Her hair is blond," but in French, German, and Russian they say "Her hairs (*cheveux, Haare, volosy*) are blond" -- dumb foreigners! Scissors are plural in English (except when people refer to "a scissor," obviously thinking of it/them as a single gadget), French (*ciseaux*), and Russian (*nozhnitsy*), but singular in German (*Schere*). Eyeglasses? Plural in Russian (*ochki*), but singular in French (*binocle*) and German (*Brille*). And ink is plural in Russian (*chernila*)!

So, if there is no logical reason why some things are thought of, in various languages, as being singular or plural, are we surprised that American kids, talking everyday English, sometimes use "wrong" forms? But are they "wrong"? Actually, sentences like "Jimmy and me's going to the movies" make perfect sense to one-half of an inseparable pair of pals. It isn't until many years later that some mean old English teacher splits up the pair by putting the two halves on opposite sides of the room and makes them say dumb (that is, "correct") things like "Jimmy and I -- or, better yet, *James* and I -- are going to the movies -- or, better yet, motion-picture theater." Teachers like this have convinced so many kids that there's something nasty about saying "Jimmy and me is" that, to this day, we hear and read statements like "I want to thank you gentlemen for taking the trouble to come to the airport to meet Mrs. Smith and I in this terrible weather." (A gracious statement, but, goodness gracious, the grammar!) They have also given a lot of people the idea that there's no difference between "no one" (as in "No one is perfect") and "none" (as in "None of us are perfect"). Why, anyone can see and hear that they're different and that "no one" is singular and "none" is plural (except when it's singular).

Or are we surprised that American kids also make mistakes recognizing plural suffixes? Perhaps the boy who showed the remains of his broken yo-yo and called it "a yo" was make-believe (it sounds just like Dennis the Menace and therefore is suspect). But I can attest to two real incidents from my own experience. When our daughter and a friend of hers were both five and were eating lunch together at our house, my wife gave them each a sandwich (cut in quarters -- without crusts, naturally), carrot sticks, and a slice of American cheese cut in strips. The little friend particularly liked the latter and asked what they were (must have been culturally deprived). "Cheese," she was told. Well, then, she asked, "May I have another chee?" (Culturally deprived, but talked polite.) Another ordinary English noun suffix tricked a nephew of mine when he was about four, many moons ago when we all went on a family picnic that included the girl destined to become his Aunt Gerry. Pointing to a plate of cherries, he asked his mother, "Can I have one of those things?" (Another one culturally deprived!) His mother said, "They're Gerry's." He said, "Well, then, can I have one of those gerries?"

Impossible, you say? Then how to you explain that the very word "cherry" itself is a mistake? When the Normans introduced the fruit to the Anglo-Saxons, the singular noun "cherise" (modern French "cerise"), meaning "one of them little red things," was misunderstood as "a lot of them little red things," since the last consonant sounded an awful lot like a plural English ending. Well, it's too late to do anything about it now. So don't go around saying, "Some joker says that we're supposed to say 'These cherrieses taste sour.'"

And look at the language now! It has words from all kinds of languages in it -- Latin, Greek, French, Russian, Italian, Indonesian. How are we supposed to know what the words really meant in the original language? Ah, that's where the plural-dropper comes in! Just as there is always a Greek expert waiting for someone to say "the hoi polloi" so that he can explain that "hoi polloi" means "the people" and, thus, "the hoi polloi" means "the the people," there are all kinds of experts telling good, solid, tax-payin' Amurricans what to do with Latin and Greek nouns in English. "You can't say 'This data seems to be correct' -- 'data' is a plural noun in Latin. Singular is 'datum,' remember?" You can argue yourself blue in the face that "data" seems to behave in two different ways. When the word means specific, isolated items of information, in scientific context, it wants to be plural: "The basic data are pressure, temperature, and humidity." But when it is used in a collective sense as a body of information, it wants to be singular: "This data was furnished by the Mayor's office." A lot of people, having talked themselves blue in the face, will avoid the issue and just say "This information was furnished by the Mayor's office." But if there is, somewhere in this country, someone who wants to fight it out to the death, like a mongoose and a cobra, here's a fact he can use: English has other nouns which, although plural in Latin, are singular in English, dammit, and nothing *but* singular. Even people who know that "opera" is the plural of "opus" do not say, "My favorite opera are 'Carmen.'" Nor do they say, "the agenda have been approved."

But there are still a few people who learned all that Latin and they're not going to let us forget it. So they write personnel regulations concerning "annual-leave maxima" ("What's the matter, 'maximums' isn't good enough for them?"). And they carefully write "these media, these

theses, these bases." Sometimes their readers figure out that those words are the plural forms of "medium, thesis, basis." Sometimes they don't. Sometimes the careful writers themselves get so careful about their pronunciation that they carry it to the point of referring to "air bases" [pronounced "base-ease"] in Western Europe." Sometimes careless readers and careless listeners pick up a catchy word but botch the ending ("This is an important media of communication," or "These are important medias of communication"). Who's going to straighten out all these bums (or is it "ba")? Why, the plural-dropper!

Formal written English being what it is, the reading plural-dropper usually pounces on a Latin word. Only an infrequent Greek boner like "this phenomena" will catch his eye. The best that he can hope for in a conversational environment is to insinuate the word "stigma" into the discussion, and wait for his partner to feed back the plural "stigmas," affording him a chance to ask, "Stigmas? Oh, I guess you mean 'stigmata?'"

As for the nonclassical languages, they are rarely encountered in contexts where one can amass a considerable number of oneupmanship points. What is he supposed to do? Tell his hostess, "These spaghetti are delicious -- 'spaghetto' is the singular of a diminutive of the noun 'spago.'" Or tell a wedding guest on the church steps after the young couple has driven away, "You have a confetto stuck onto your cheek -- 'confetti' is a plural form, you know." Or is he supposed to point to the sign on the cafeteria counter that reads "Lasagna 70 cents" and ask the server, "Certainly that can't be right? 'Lasagna' is the Italian word meaning '*a* noodle.' Certainly we get more than '*a*' noodle for 70 cents? Is it conceivable that it's a misspelling for 'lasagne,' the proper plural form?" What's he supposed to do when he sees a recipe in the newspaper for "pirozhki" that -- in addition to leaving out the mushrooms! -- says, "Each *pirozhki* should be bite-size"? Should he write a nasty letter to the editor, signing it Paul E. Glott or some other silly name, and say, "Anyone with a modicum of knowledge of Russian haute cuisine should be aware of the fact that the singular of 'pirozhki' is 'pirozhok.'"

Certainly he's supposed to do none of these things. He's supposed to *avoid the issue*, like a chicken mongoose. (Not a mongoose that eats chickens -- they're brave -- but a mongoose who won't fight a cobra -- they're chicken!) He's supposed to smile understandingly at other people's mistakes and make sure that when he uses such words himself, they can be interpreted either in the singular or the plural. He would, in a *Newsletter* item, for example, say, "Smalti can be used in such-and-such a way," rather than "Smalti is used" or "Smalti are used." In effect, he ideally should write just like the zoo owner ordering two mongooses. "'Please send me two mongooses.' No, strike that out -- make it 'two mongeese.' No, strike *that* out. Make it, 'Please send me one mongoose as soon as possible. And, oh, by the way, while you're at it, send me another one."

(U)

Letter to the Editor

To the Editor, CRYPTOLOG:

In reply to [redacted] article, "Whither the SRA?" (CRYPTOLOG, September 1977), I would like to say that some of my best friends were SRAs (whatever *that* is)! Back in the PCP days (pre-career panel), the relationship between TA and IRA (as it was then called) was quite clear: if you were below a certain grade (I think it was GS-9), you were TA, and if you were above that grade, you were IRA. We thought of IRA as professional (with a small p) and TA as preprofessional and that was the way the job auditors titled the jobs. Then one day the career panels were formed, and when the dust cleared, behold -- TA and IRA were two separate fields!

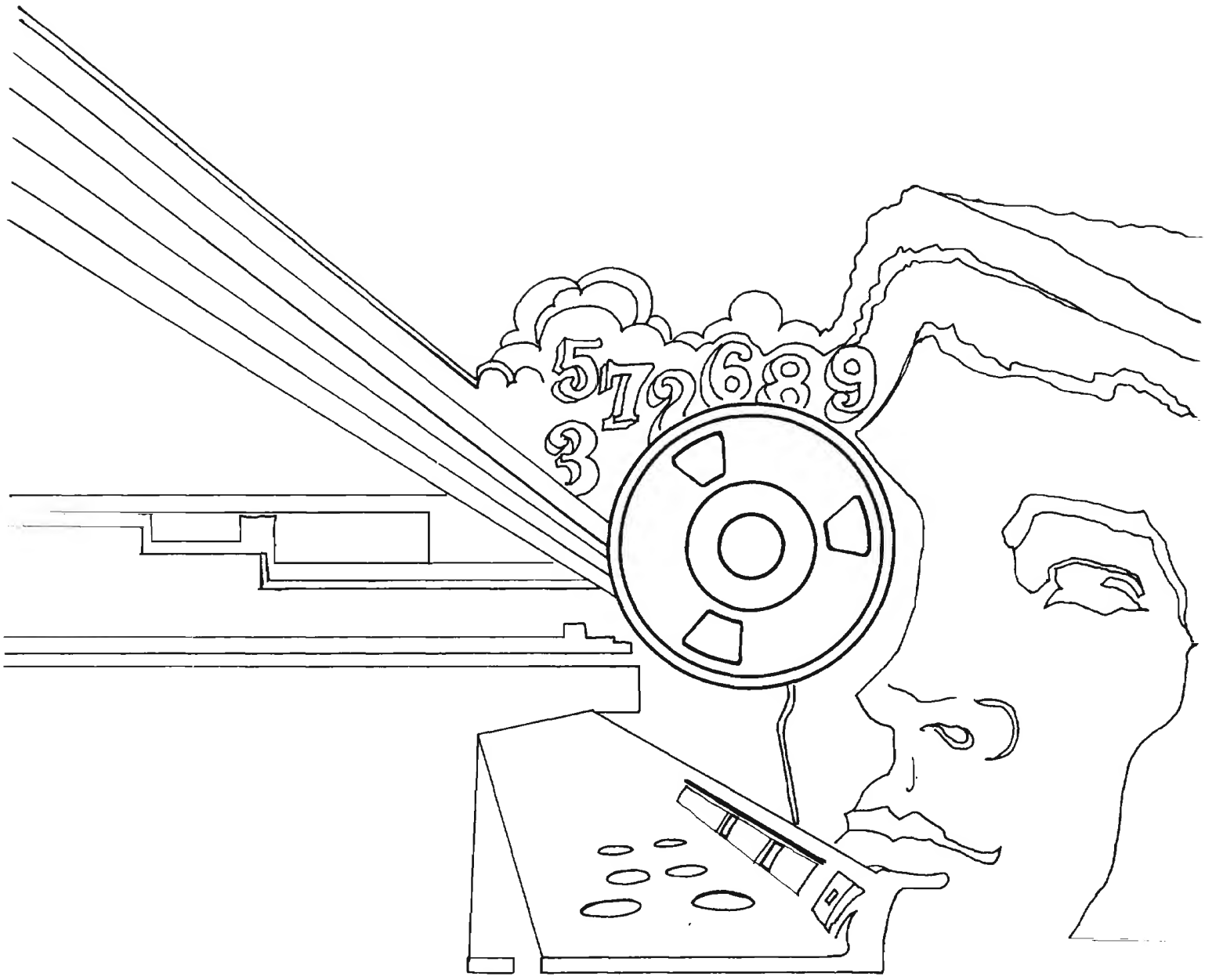
We (in that early TACP) studied the situation at great length and found, among other things, that it was then standard practice for job auditors to classify a job as IRA if the incumbent produced *any* reports and TA if he or she didn't. As I recall, we did not care for that at all, since it was our view that *all* traffic analysis efforts should be aimed ultimately at the production of results in writing, i.e., reports. And, after some negotiation, the job auditors' guidelines were adjusted.

Last, but clearly not least, the two career panels were directed to investigate the problem of "defining the boundary line" between them. After some 6 months of discussion, it was concluded that the boundary was indeed a problem. What we finally committed to paper said, in effect, that at one end of the spectrum there were jobs that were clearly TA, and at the other end there were easily recognizable IRA jobs, but that all along the line between those two extremes there was overlap between the two fields.

My own view is that reporting (to consumers) can be a very specialized business and undoubtedly is a cryptologic skill but it is really more of an *overlay* skill, like supervision. The field seems to have drawn most of its people from the language and traffic analysis fields (many of the better reporters I've known began either as a linguist or as a traffic analyst).

Finally, what traffic analysis is all about is producing intelligence -- by reconstructing the network, by recovering the signal plan, by watching the target day after day to see what it is doing and how today's behavior differs from yesterday's.

[redacted] Chief, Traffic Analysis
Office of Techniques and Standards (U)


5 7 2 6 8 9
3